Carey Rodriguez Milian, LLP
David P. Milian*
dmilian@careyrodriguez.com
John C. Carey*
jcarey@careyrodriguez.com
Jennifer M. Hernandez*
jhernandez@careyrodriguez.com
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Telephone: (305) 372-7474
Facsimile: (305) 372-7475
*Admitted *pro hac vice*

Bottini & Bottini, Inc.
Albert Y. Chang (SBN 296065)
7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
Telephone (858) 914-2001
Facsimile: (858) 914-2002
Email: achang@bottinilaw.com

Counsel for Plaintiff Clayton P. Zellmer

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CLAYTON P. ZELLMER,

Plaintiff,

vs.

FACEBOOK, INC.,

Defendant

CASE NO. 3:18-CV-01880-JD

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

Class Action

Date: July 8, 2021
Time: 10:00 a.m.
Location: Courtroom 11, 19th Floor
Judge: Hon. James Donato
Trial Date: April 11, 2022
Complaint Filed: March 27, 2018

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Pursuant to Rule 56 of the Federal Rules of Civil Procedure and this Court's Standing Order for Civil Cases, Plaintiff hereby opposes Defendant Facebook, Inc.'s ("Facebook") Motion for Summary Judgment (ECF No. 67) ("MSJ").

I. BACKGROUND

A. Facebook's Course of Conduct

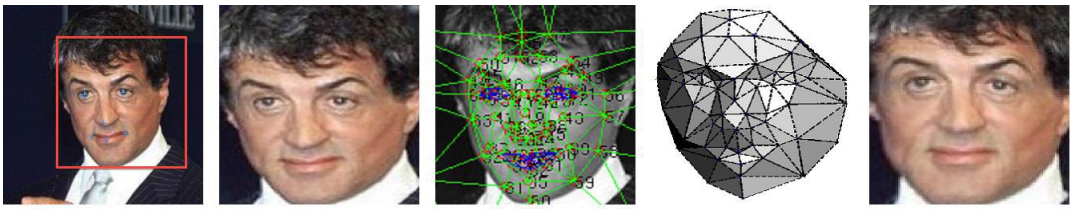
Facebook encourages users to fill their Facebook pages with personal information, generating reams of data for Facebook to mine, sort, aggregate, disaggregate, and sell. One of the principal sources of such information is the torrent of photos users upload daily.[1] Until just recently, starting in June 2011, virtually every uploaded photo from Illinois has been immediately subjected to Facebook's facial-recognition software. [redacted][4] Facer's source code unequivocally demonstrates that Facebook creates, collects, and obtains the biometric identifiers of non-users, like the Plaintiff.[5]

The scanning of faces commences upon the initial upload of a photo. At the time of upload, Facebook knows: [redacted];[6]

[1] Facebook, Inc, Registration Statement (Form S-1), at 74 (Feb. 1, 2012) ("[M]ore than 250 million photos *per day* were uploaded to Facebook in the three months end[ing] December 31, 2011.").
[2] FBBIPA_0001123-0001125, Ex. 1. All "Ex._" references are to exhibits filed with this response.
[3] Ex. 2, excerpts from the Deposition of Robert Sherman ("Sherman Dep.", at 228:9-21; Ex. 3, excerpt from Taigman Dep., at 176:9-20, 273:13-17, Ex. 4, FBBIPA_0009297-9298; Ex. 5, FBBIPA_00028668; Ex. 6, Sworn Declaration of Dr. Atif Hashmi attaching expert Report dated December 22, 2017 ("Hashmi Dec. Report") at p. 15-24; 26-27. All emphasis is added unless otherwise stated.
[4] Ex. 3, Taigman Dep. at 172:1-2.
[5] Ex. 6, Hashmi Dec. Report, p. 19 at ¶45; *Id.* Hashmi Dec. Report, p. 24 at ¶¶ 52-53.
[6] Ex. 7, excerpt from the October 10, 2017, Deposition of Dan Barak ("Barak Dep."), at 230:11-232:7.

[redacted].[10] Facebook furthers its business objectives by stripping and processing as much data from each uploaded photo that it possibly can.

The figure below illustrates the first steps performed by Facebook's facial recognition pipeline-- any one of which constitutes scanning of face geometry.[11]

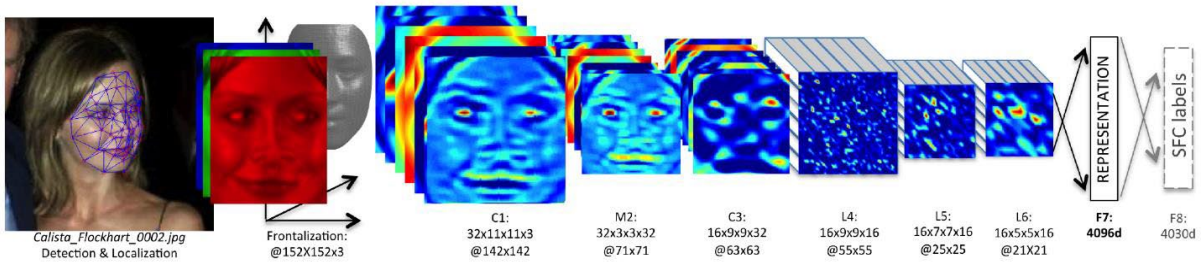


(a) (b) (c) (d) (e)

This aspect of Facer's face scanning pipeline "[redacted]

[7] Ex. 3, excerpt from the Taigman Dep., at 316:13-319:15; *supra* Ex. 2, excerpt from the Sherman Dep., at 358:12-359:18.
[8] Ex. 7, excerpt from the Barak Dep., at 153:3-19.
[9] Ex. 8, FBBIPA_00001011;
[10] Ex. 9, FBBIPA_00043017 [redacted]
[11] Ex.6, Hashmi Dec. Report, p.6-7; Ex. 12, McCoy Dep. at p. 87:3-25.
[12] Ex. 6, Hashmi Dec. Report, p. 19 at ¶ 4.

[redacted]



[redacted]

[13] Ex.6, Hashmi Dec. Report, p. 19 ¶ 45.
[14] Ex. 6, Hashmi Dec. Report, p. 20 ¶ 47.
[15] Ex. 6, Hashmi Dec. Report, p. 20 ¶ 48.
[16] Ex. 6, Hashmi Dec. Report, p. 22-23 ¶¶ 50–51.
[17] *Id.*
[18] Ex. 6, Hashmi Dec. Report, p. 24 ¶ 52.

[redacted]

Facebook's technical paper "Deep Face" confirms that Facebook processes and collects scans of face geometry for non-users by processing non-user's images in precisely the same manner as the images of users. In 2014, Yaniv Taigman[20], along with colleagues at Facebook Artificial Intelligence group, published a paper titled "Deep Face: Closing the Gap to Human-Level Performance in Face Verification." Ex.13. The system utilizes "deep learning," using large data sets of photographs to train the system to recognize faces. Ex.13 at FBBIPA_0001214. The DeepFace paper all but admits that what Facebook describes as its face alignment pipeline, particularly the "face detection" tier, is dependent on a scan of face geometry from uploaded photographs. *Id*. at FBBIPA_0001215. "[A]lingment is based on using fiducial point detectors to direct the alignment process." *Id*. Each time a fiducial point detector is applied, "fiducial points are extracted by a Support Vector Regressor (SVR) trained to predict point configurations from an image descriptor." *Id*. at FBBIPA_0001216 (describing "6 fiducial points" identified in first step of alignment phase as "center of the eyes, tip of the nose and mouth location"). Facebook's "network architecture is based on the assumption that once the alignment in completed [illustrated in the first figure on p. 4 *supra*], the location of each facial region is fixed at the pixel level." [21]

[19] Ex.6, Hashmi Dec. Report, p. 26 ¶ 60.
[20] Facebook designated Yaniv Taigman as its Rule 30(b)(6) representative in the related *Gullen* and *In Re Facebook Biometric Information Privacy Litigation* cases. Case No. 3:16-cv- 00937 JD and 3:15-cv-03747-JD.
[21] Ex. 13, FBBIPA_0001214-17.

A. Facebook Stores Face Recognition Data Associated With Non-Users' Faces

Facebook maintains an active database that permanently stores face recognition data associated with photo uploads and photo sharing for users and non-users alike.[22] The data associated with Plaintiff's face depicted in photos uploaded on June 3, 2013, January 20, 2018, and October 12, 2020, [redacted]

[22] Ex.12, McCoy Dep. at p. 19:13-24;26:
[23] Ex.12, McCoy Dep. at p. 19:8-12; 20:2-20; 22:7-11;25:13-16; 26:3-21; 27:5-27; 28:3-17; 31:23-25,32:1-5; 32:19-22; Ex.14, Zellmer 0003, 00009, 00010, 00011.
[24] Ex.12, McCoy Dep. at p. 25:13-16;
[25] Ex.12, McCoy Dep. at p. 42:14-25; p. 43:1-7 [redacted]
[26] Ex.12, McCoy Dep. at p. 32:19-22; p. 33:7-20 [redacted]
[27] Ex.12, McCoy Dep. at p. 33:7-20.
[28] Ex. 12, McCoy Dep. at p. 47:10-17.
[29] Ex. 12, McCoy Dep. at p.47:5-7.

[redacted]

B. Facebook Obtained Plaintiff's Biometric Identifiers

Plaintiff's face was processed through Facer's facial recognition pipeline, with each stage of the pipeline scanning Plaintiff's face geometry. [redacted][34] Facebook continues to collect, use, and possess the biometric identifiers of Illinois residents who are not Facebook users.

C. The Illinois Biometric Information Privacy Act

The foregoing course of conduct – Facebook's surreptitious scanning of face geometry from Illinois residents' who have never had a Facebook account --poses precisely the threat to individual privacy that motivated the Illinois legislature to enact BIPA, 740 Ill. Comp. Stat. 14. Specifically, §15(b) of BIPA provides that absent prior notice and consent by the affected person or the person's legally authorized representative "[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric

[30] Ex. 12, McCoy Dep. at p. 46:8-17.
[31] Ex. 12, McCoy Dep. at p. 44:7-20.
[32] Ex. 12, McCoy Dep. at p. 46:8-17.
[33] Ex. 14, Zellmer 00011
[34] Ex. 12, McCoy Dep. at p. 45:8-14.

identifier or biometric information[.]" *Id*. at 14/15(b). The definition of "Biometric identifier," includes a "scan of …face geometry." *Id*. at 14/10.

Section 15(a) compels any private entity in "possession of biometric" data to "develop a written policy, *made available to the public*, establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." *Id.* at 14/15(a) The purpose of this provision is to enable a member of the public to obtain notice concerning a particular company's procedures.

As more fully discussed below, Facebook's MSJ seeks to redefine the term "biometric identifier" by engrafting a limitation that would permit the unconsented-to collection of biometric identifiers unless "used to identify an individual." MSJ at 11. Reading in such qualifying language would erroneously conflate the statutory definitions of biometric identifier with biometric information. Facebook also argues that it is exempt from liability because it does not *at least temporarily* retain or control biometric data of non-users. (MSJ 16). This argument ignores that Facebook holds and exercises control over non-users' biometric data to such an extent that it creates and compares the unique face signatures of non-users against the faces signatures of at least 220 others stored on Facebook's system. [redacted]

Facebook concedes that it failed to comply with BIPA's notice and consent requirements under 740 ILCS 14/15(b).[35] Facebook argues that it should be exempted because obtaining informed consent from non-users is impossible. As discussed below, BIPA is not a strict liability statute. Companies are held liable if they act negligently, intentionally, or recklessly. 740 ILCS

[35] Requiring private entities to "inform the subject or the subject's legally authorized representative in writing" that biometric data is being collected or stored, the specific purpose and length of term for which biometric data is being used, and obtain a written release by subject or the subject's legally authorized representative.

14/20 (1)(2).[36] Conversely, companies exercising reasonable care are not liable under BIPA, even if compliance regimes are not 100% fail-safe. Facebook can exercise reasonable care and comply with BIPA's notice and consent requirements without abandoning face scanning in Illinois altogether by implementing any one of several alternative procedures.[37] If, however, Facebook continues to *falsely* pretend that it is helpless, then it should refrain from scanning photos uploaded from Illinois, [redacted].[38]

The MSJ fails to address Plaintiff's 15(a) claim.[39] As "[a] private entity in possession of biometric identifiers or biometric information," Facebook cannot legitimately dispute that it failed to "*develop a written policy, made available to the public*, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information *when the initial purpose for collecting or obtaining such identifiers* or information has been satisfied…." 740 ILCS 14/15(a). Compliance with §15(a) would have alerted Illinois residents, users and non-users alike, about Facebook's face scanning practices, including the length of time Facebook retains such data. Compliance would have required Facebook to publish policies for retaining and destroying biometric data. Because the MSJ does not address Plaintiff's claim under 15(a), the claim should proceed to trial.

As the Illinois Supreme Court made clear: a person is "aggrieved" by a violation of BIPA whenever "a private entity fails to comply with one of section 15's requirements," because "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person …whose biometric identifier…is subject to the breach." *Rosenbach v. Six Flags Entertainment*

---

[36] Liability attaches against companies that act "negligently" "intentionally" or "recklessly."

[37] *See,* https://www.amazon.com/gp/help/customer/display.html?nodeId=201376540, Amazon Photos Terms of Use for Illinois Residents, §6.6 (Last accessed June 4, 2021)

[38] Ex. 15, FBBIPA_00008877([redacted]) Ex. 16, FBBIPA 0036806 [redacted] ; Ex. 17, FBBIPA_00036832 [redacted]

[39] Complaint ¶ 27 (ECF No. 1)

Corporation 129 N.E. 3d 1197, 1206 (Ill. 2019). Facebook violated Plaintiff's statutory rights and the rights of non-users. Facebook's MSJ fails.

II. LEGAL STANDARD

Summary judgment is only appropriate "when no genuine and disputed issues of material fact remain, and when, *viewing the evidence most favorably to the nonmoving party,* the movant is clearly entitled to prevail as a matter of law." *Satterfield v. Simon & Schuster, Inc*., 569 F.3d 946, 950 (9th Cir. 2009)(citing Fed. R. Civ. P. 56). A material issue of fact is a question the jury must answer under the applicable substantive law, and a dispute is genuine "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc*., 477 U.S. 242, 248 (1986). "Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge." *Id*. at 255

III. FACEBOOK IS NOT ENTITLED TO SUMMARY JUDGMENT

Facebook's MSJ makes four fact-specific arguments: (1) that scans of face geometry must be used to identify an individual for statutory liability to attach, even though the definition of "biometric identifier" contains no such qualifier and data stored in Facebook's databases can be used to identify an individual; (2) that Facebook never collected, captured, or otherwise obtained Plaintiff's biometric identifiers, even though Facebook created and stored Plaintiff's biometric identifiers, including his unique face signatures, and took the time to compare Plaintiff's biometric identifiers against its database of face signatures and face templates; (3) that Facebook cannot figure out how to comply with BIPA's notice and consent requirements, even though compliance requires reasonable care and other companies with photo sharing services substantially identical to Facebook's easily comply, and; (4) that Plaintiff is not entitled to injunctive relief, even though BIPA expressly provides for injunctive relief under the precise facts present here. *See*, 740 ILCS 20 (4). A reasonable jury could, indeed should, find for Plaintiff on each of these arguments. Facebook's MSJ must be denied.

A. Facebook Concedes That Face Signatures Constitute "Scans of Face Geometry" as Defined Under BIPA

Facebook concedes, for purposes of its MSJ, that face signatures are "scans of …face geometry."[40] Because the definition of "biometric identifier" includes a "scan of … face geometry" Facebook has necessarily conceded that Plaintiff's face signatures constitute "biometric identifiers." Facebook's concession removes from dispute, for now, what the record evidence makes plain: that the unique face signatures Facebook collects are "biometric identifiers" as defined under 740 ILDC 14/10. Thus, whether the face signatures Facebook generated are "biometric identifiers" under BIPA is a question of fact for the jury.

B. Facebook is Subject to BIPA Because it Obtains Biometric Identifiers

In enacting BIPA, Illinois banned unauthorized gathering of two distinct and separately defined things: (1) "biometric identifiers," which are defined as retinal scans, iris scans, voiceprints, fingerprints, and scans of hand or face geometry; and (2) "biometric information," i.e., any information based on a biometric identifier "used to identify an individual." Facebook collects, captures, uses or otherwise obtains biometric identifiers – specifically, scans of face geometry – from people who do not have a Facebook account without their consent. Facebook therefore violates the statute.

Facebook's MSJ does not contest that a face signature is a "biometric identifier." It also does not dispute that Facebook created Plaintiff's face signatures without his consent. Instead, Facebook argues that scans of face geometry are not subject to BIPA regulation unless they are "used to identify an individual." MSJ at 11. Facebook's argument fails because the requirement that data be "used to identify an individual" pertains only to the definition of biometric information, not biometric identifier. Scans of face geometry are biometric identifiers, not biometric information. 740 ILCS 14/10. Facebook's contention, if adopted, would require the Court to add limiting conditions to the definition of biometric identifier that the Illinois legislature chose to exclude.

---

[40] MSJ, p. 11, fn. 6 "Facebook's position is that neither a face signature nor template is a "scan of face geometry" within the meaning of BIPA, ***but it is not seeking summary judgment on that ground***."

i. Facebook improperly conflates the definitions of "biometric identifier" and "biometric information."

In this case, the definitions of "biometric identifier" and "biometric information" differ at exactly the point where Facebook has placed all its chips.

Section 10 of BIPA states:

> 'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. . . .
>
> 'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

740 Ill. Comp. Stat. 14/10. By processing Plaintiff's face through its detection, alignment, and representation pipeline, Facebook scanned Plaintiff's face geometry. It used Plaintiff's face scans to create and compare Plaintiff's unique face signature against the faces of others. Facebook thus collected Plaintiff's biometric identifier in violation of BIPA. Facebook's argument, that the data it collected are not subject to BIPA "because they are not used to identify an individual," is wrong. MSJ 11–15. BIPA does not restrict regulation of scans of face geometry (i.e. biometric identifiers) to scans that are used to identify a person. Rather**,** the Illinois legislature defined biometric information as "any information regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. By contrast, biometric identifier contains no such limitation or qualification. *Id.* Biometric identifier means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.*

ii. Facebook's Argument Ignores Canons of Statutory Construction

"When faced with questions of statutory construction, 'we must first determine whether the statutory text is plain and unambiguous' and, '[i]f it is, we must apply the statute according to its terms." *Banko v. Apple, Inc.*, 20 F. Supp. 3d 749, 755 (N.D. Cal. 2013) (alterations in original). Here, the statutory definitions are unambiguous. The meaning of a biometric identifier is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." There is no ambiguity on

this point, nor does Facebook argue that one exists. "If the statutory text is unambiguous, the inquiry begins and ends with the text." *Id.* (citing *BedRoc Ltd. v. U.S.*, 541 U.S. 183 (2004)).

Facebook's conflation of the definitions of "biometric identifier" and "biometric information" to include a requirement that all biometric identifiers be used to identify an individual is contrary to canons of statutory construction. "The preeminent canon of statutory interpretation requires us to 'presume that [the] legislature says in a statute what it means and means in a statute what it says there.'" *BedRoc Ltd., LLC v. U.S.*, 541 U.S. 176, 184 (2004) (alterations in original) (quoting *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253–54 (1992)). Indeed, the 9th Circuit has repeatedly held that:

> It is a well-established canon of statutory interpretation that the use of different words or terms within a statute demonstrates that Congress intended to convey a different meaning for those words. Congress's explicit decision to use one word over another in drafting a statute is material. It is a decision that is imbued with legal significance and should not be presumed to be random or devoid of meaning.

Pit River Tribe v. Bureau of Land Management, 939 F.3d 962, 970–71 (9th Cir. 2019) (quoting *SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003)). Here, the legislative decision to separately define "biometric identifier" and "biometric information" makes clear that the definitions are not interchangeable nor may limiting language from one definition simply be engrafted on another. Moreover, the decision to include this limitation to define biometric information and yet exclude it from the definition of biometric identifier in the immediately preceding paragraph, must be afforded substantial legal significance. The Illinois legislature could not have intended for a face scan to be a "biometric identifier" only if "used to identify an individual." Rather, the legislature was clear that a "scan of . . . face geometry" ***is*** a biometric identifier, full stop.

Moreover, "[w]hen [the legislature] includes particular language in one section of a statute but omits it in another section in the same Act, it is generally presumed that [it] acts intentionally and purposely in the disparate inclusion or exclusion." *Id.* at 971 (quoting *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 452 (2002)). The legislature acted intentionally by defining biometric information as data used to identify an individual. The legislature explicitly excluded that precise requirement from the definition of biometric identifier. Having used the precise language

Facebook contends defines both types of biometrics to define only one type of biometric data, it must be presumed that the legislature's choice was intentional. The Illinois Supreme Court is equally clear on this point. "Our rules of statutory construction do not permit us to add new limitations [to a statute] that the legislature did not specifically enact." *Cassidy v. China Vitamins*, LLC, 120 N.E. 3d 959, 966 (Ill. 2018).

Facebook relies on an Illinois Attorney General's opinion (MSJ 12) that "biometric identifiers" are "commonly understood" to refer to "measurements and analysis…that identifies a person." 2017 WL 10084298 (Ill. A.G.). The opinion, issued in the context of a Freedom of Information Act ("FOIA") request, admits that neither FOIA nor Illinois statutes define the term for purposes of FOIA. *Id.* at *3. By contrast, BIPA defines "biometric identifier" to include "a scan of …face geometry" and nowhere is the definition limited to data "used to identify an individual." BIPA's definition, not the Illinois Attorney General's opinion, governs the case.

Facebook's reliance on *Patel v. Facebook, Inc.,* 932 F. 3d. 1264 (9th Cir. 2019), (MSJ at 13) is also misplaced. As this Court will recall, *Patel* affirmed this Court's ruling on Article III standing and class certification, which found that a person is aggrieved and has standing under BIPA by virtue of a violation of the person's statutory rights. *Patel* does not address the definition of biometric identifier much less hold that BIPA's reach is limited to scans of face geometry used to identify an individual. Facebook's reliance on *Mutnick v. Clearview AI, Inc.,* 2020 WL 4676667 (N.D. Ill. August 12, 2020), a slip opinion addressing a motion to dismiss for lack of personal jurisdiction and to transfer venue, is equally unavailing. Facebook's MSJ merely quotes the *Mutnick* court's paraphrasing of the allegations in a complaint. (MSJ 14) The *Mutnick* opinion neither infers nor holds that BIPA's regulatory provisions apply only when scans of face geometry are used to identify an individual. *Id.* at *3-4.

By contrast, *Hazlit v. Apple, Inc.,* 500 F. Supp. 3d 738 (S.D. Illl. 2020), addresses the definitional distinctions between "biometric identifier" and "biometric information" and firmly supports Plaintiff's position:

> The definition of biometric identifier explicitly includes scans of face geometry, which Plaintiffs allege Apple collected without consent. Apple reads the word "identifier" to exclude data that does not identify an actual person. This Court finds that interpretation too narrow.

Id. at 749.

Finally, even if Facebook's definition conflation was appropriate, Facebook indeed maintains biometric data that can identify an individual. Plaintiff's face depicted in photos uploaded on June 3, 2013, January 20, 2018, and October 12, 2020, [redacted] Unlike biometric information, scans of face geometry need not be used to identify an individual to be regulated under BIPA. Nevertheless, the data Facebook obtains do just that. Facebook's MSJ must be denied.

C. Facebook Violated BIPA by Collecting, Capturing or Otherwise Obtaining Plaintiff's Biometric Identifiers.

Facebook argues that it does not retain control of non-users' biometric identifiers and therefore it should escape liability as a matter of law. (MSJ 16). Facebook's argument rests on the premise that by scanning non-users' faces, creating face signatures, and attempting to match non-users' face signatures against hundreds of others, Facebook does not hold the data for a *long enough* time to matter. Facebook's MSJ misstates the facts and misapprehends the law.

BIPA extends to all private entities who "collect" "capture" "receive through trade" or "otherwise obtain" a person's biometric identifiers. 740 ILCS 14/15(b). Facebook argues that

[41] Ex. 12. McCoy Dep. at p 42:14:25;43:7.
[42] Ex. 12, McCoy Dep. at p. 19:8-12; 20:2-20; 22:7-11;25:13-16; 26:3-21; 27:5-27; 28:3-17; 31:23-25,32:1-5; 32: 19-22; Ex. 14, Zellmer 0003, 00009, 00010, 00011

each of the above terms "connotes at least *temporary* retention of, and *control* over, the data." (MSJ 16). It then argues that the length of time it retains biometric data is somehow not temporary. But Facebook's practices more than satisfy the "temporary retention and control" standard it advocates in its MSJ. [redacted][45] Having argued that *temporary* retention and control satisfies BIPA's requirements, Facebook advocates a standard that it comfortably meets.

Facebook then suggests, without evidence, that non-users' biometric data are immune from risk and are therefore undeserving of BIPA's protections. (MSJ 16). In truth, the risks to Illinois non- users' privacy is no less real than the risks to Illinois users, to whom Facebook has agreed to pay $650 Million.[46] Nothing prevents a cyber intruder from burrowing into Facebook's systems and intercepting Plaintiff's biometric identifiers at any point in the face scanning pipeline.[47] The advances in technological tools available to hackers and their sophistication level

[43] Ex. 6, Hashmi Dep. Tr. 283:5-19.
[44] Ex. 6, Hashmi Dec. Report, p. 19, ¶ 45.
[45] Ex. 6, Hashmi Dec. Report, p. 24, ¶52.
[46] *In Re Facebook Biometric Privacy Litigation,* Case No. 3:15-cv-03747-JD (D.E. 537).
[47] *New Data Breach Has Exposed Millions of Fingerprints And Facial Recognition Records: Report* (Forbes, August 14, 2019). https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=1f55217c46c6 (last accessed June 5, 2021).

continue to grow exponentially.[48] The Court should not accept, especially on summary judgment, Facebook's invitation to tie BIPA's protections to an arbitrarily contrived duration test. As the Illinois legislature observed: "The full ramifications of biometric technology are not fully known."[49] The full ramifications of advances in technology available to hackers now or in the future are also not fully known. The Illinois legislature enacted BIPA because the public's welfare "will be served by regulating the *collection, use, safeguarding, handling*… of biometric identifiers and information."[50] BIPA regulates Facebook's collection, use and handling of Plaintiff's biometric identifiers, no less than any other biometric identifiers. Finally, the risks to non-users' privacy from Facebook's face scanning practices is a complex question of fact, the ultimate adjudication of which could benefit from expert testimony.[51]

Facebook's authorities are inapposite. In *Heard v. Becton, Dickinson & Co*., 440 F. Supp 3d 960 (N.D. Ill. 2020), the plaintiff sued the manufacturer of fingerprint scanning devices sold to plaintiff's employer. The plaintiff failed to allege how the manufacturer—in contrast to his employer-- "collected" plaintiff's finger scans for purposes of alleging a violation of §15(b). *Id.* at 966. The court stated that an entity must take some "active step" in order to "collect." *Id.* Turning to the plaintiff's §15(a) and 15(d) claims the complaint failed to allege that the manufacturer had "possession" because there was no allegation that the manufacturer exercised *any* dominion or control over plaintiff's data. *Id.* Here, Facebook repeatedly "collected," "captured" or "otherwise obtained" Plaintiff's face scans, going so far as to create and compare Plaintiff's unique face signatures to Facebook's users and the users' 220 friends on at least four separate occasions. Facebook is liable under §15(b). Facebook also exercised dominion and control over Plaintiff's biometrics, thus making clear Facebook's responsibility for complying

---

[48] *Hack Suggests New Scope, Sophistication for Cyberattacks* (Wall Street Journal, December 17, 2020); ("The attack blended extraordinarily stealthy tradecraft, using cyber tools never before seen in a previous attack…") https://www.wsj.com/articles/hack-suggests-new-scope-sophistication-for-cyberattacks-11608251360 (last accessed June 5, 2021).

[49] 740 ILCS 14/5 (f).

[50] 740 ILCS 14/5 (g).

[51] Expert Disclosures are due August 23, 2021 (D.E. 63). Plaintiff intends to retain a cyber security expert.

with §15(a)'s public notice requirements.[52] Indeed, Facebook's control over the data is so complete that Plaintiff's biometric identifiers did not even exist until Facebook created them.

D. Facebook Can Comply

In its final attempt to find an escape hatch, Facebook latches on to the meritless argument that compliance with BIPA is impossible. Facebook's assertion is false and premised on a plethora of disputed facts.

i. BIPA Proscribes Negligent, Reckless, or Intentional Conduct - Reasonable Efforts to Comply Are Required

"As noted earlier, the Privacy Act only subjects violators to statutory damages if there is negligence or willfulness. 740 ILCS 14/20. So even if the Plaintiffs' construction of the Act were to depend on a totality-of-the-circumstances test for assessing location, [Facebook] could conceivably avoid liability by taking reasonable steps toward compliance." Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1104 (N.D. Ill. 2017). BIPA is not a strict liability statute—compliance requires reasonable conduct.

ii. Consent Can Be Obtained From the Subject or An Authorized Representative.

Section 15(b) permits private entities that traffic in biometrics the ability to obtain consent directly from the affected person or indirectly from the person's authorized representative. *See* 740 ILCS 14/15 ("No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative…."). 740 ILCS §15(b)(1)-(3).

iii. Facebook Can Get Electronic Affirmation That the User Obtained Consent of the Persons Depicted in Photos

Prior to uploading a photo in Illinois, Facebook could prompt the Illinois user to acknowledge/affirm that the photo the user is about to upload contains only the face of the user. Upon confirmation, facial recognition could be applied. This simple procedure would avoid the

[52] As previously discussed, Facebook's MSJ does not address Plaintiff's §15(a) claim, which is the only BIPA claim in this action requiring "possession."

negligent or intentional scanning of un-consenting non-users while preserving the ability to collect biometric data from consenting users. A failure to check "yes" would still permit the photo to be posted to the user's account; however, facial recognition would not be run for that photo. Similarly, Facebook could prompt the Illinois user to affirm that the photo the user is about to upload contains the users' face and /or only the faces of others whom the user has verified are also Facebook users. Either of these procedures would not require Facebook to cease face scanning in Illinois. It would, however, put Facebook in compliance with BIPA because Facebook would be taking reasonable steps (*i.e.* not acting negligently) to avoid scanning non-users without consent. Had Facebook implemented compliance procedures like these before it began collecting face scans by the billions, it would have engaged in reasonable, non-negligent, efforts to comply, which is exactly what the statute requires.

iv. Other Companies With Photo Services Comply; So Can Facebook

Alternatively, Facebook could publish updated terms of use directed to existing Illinois users pursuant to which users are required to affirm that by choosing to have face scanning "on," the user has obtained written permission to apply face scanning from every person depicted in the photo. This is precisely how companies like Amazon, with identical photo sharing and storage services, comply. Amazon Photos terms of use illustrate the point:

> 6.6 **Notice to Illinois Residents**. The image recognition features of the Services are not initially enabled for residents of the State of Illinois. If you are an Illinois resident and (a) wish to use the image recognition features of the Services … you understand that image recognition analysis will be performed on the photos stored in your account or that are contributed by you to the Family Vault, and you represent to us that you have obtained the informed written consent of the individuals in the photos stored in your account permitting us to use image recognition analysis on photos of them. If you are an Illinois resident, you are also required to read and agree to the important legal information regarding your use of such features here.[53]

Likewise, Facebook could disable facial recognition for Illinois residents and require users to affirm, as a condition for re-enabling face scanning for that particular account, that the user has

[53] https://www.amazon.com/gp/help/customer/display.html?nodeId=201376540 (last accessed June 4, 2021).

obtained the informed written consent of the individuals in the photos.[54] The same notice could have the user affirm that the user will disable face scanning when uploading photos for which the non-user has not provided consent. By implementing these procedures, Facebook would be taking reasonable care to comply with BIPA.

Like Amazon, Shutterfly Inc., has agreed to implement a BIPA-compliant notice and consent procedure for its photo sharing service directed to non-users. Shutterfly will disable facial recognition for customers located in Illinois and require the Illinois user to affirmatively check "yes" to re-enable the feature. The user must also represent that by enabling facial recognition, "you are representing to us that you have obtained consent for the [Face Grouping] feature from the people who appear in your photos or, if they are under the age of 18, from their parents or legal guardian."[55]

Facebook argues that notice and consent compliance is not required here because BIPA is not intended to protect the privacy interests of individuals (MSJ 19) whose biometrics are not permanently stored. As support, Facebook offers an inapt hypothetical. (MSJ 19-20) Facebook asks us to imagine that a company has chosen to use facial recognition technology to screen employees for access to sensitive areas of an industrial site. It then asks us to imagine that an intruder gains entry to the restricted area resulting in the company scanning the intruder's face. Facebook contends that "[u]nder Zellmer's reading of the statute, the company would be liable under BIPA to the would-be intruder for analyzing his face." MSJ 20. First, Facebook's hypothetical erects a strawman-- Plaintiff has never read BIPA in a way that would impose liability under any scenario like the one Facebook posits. Second, because BIPA proscribes

[54] Facebook has already agreed, as a condition of settlement in *In Re Biometric Information Privacy Litigation,* to turn off face recognition and delete biometric data it collected unless the Illinois user provides informed consent to turn it back on. *In Re Biometric Information Privacy Litigation,* Case no. 3:15-cv-03747-JD (D.E 517 at 22). Clearly, activating or deactivating face scanning based on whether a user checks a box to affirm compliance is a reasonable method of obtaining consent. Unless Facebook requires the user to affirm that they obtained the informed consent of all the individuals depicted in future photo uploads, or allows face scanning of photos the user affirms contains only users' faces, Facebook will continue to violate the statutory rights of non-users.

[55] Ex. 18, "Notice to Illinois Users-Face Groupings," submitted as part of a class action settlement of user and non-user BIPA claims in *Miracle-Pond et. al. v. Shutterfly*.

negligent or intentional conduct, under no rational reading of the statue would the employer/property owner be liable (*i.e*. negligent) for failing to obtain the consent of someone whose face was scanned while that person engaged in criminal trespass. Unlike the unwelcomed intruder, Facebook intentionally invites its Illinois users to upload photos containing faces of non-users without providing the opportunity to obtain their consent. Facebook then scans non-user's faces, creates and uses their biometric identifiers to advance Facebook's business interests, and even permanently stores data associated with the non-users faces.

Next, Facebook attempts to advance its MSJ by cherry picking excerpts from Mr. Zellmer's deposition, and in so doing completely mischaracterizes his testimony. Mr. Zellmer did not testify that his goal in filing this lawsuit is to force Facebook to halt face scanning altogether. Rather, he testified that he wanted Facebook to comply with the statute; but as a lay person who is not technically savvy, he could not offer Facebook advice on how it might legally comply.

> Q: Mr. Zellmer is one of the things that you want Facebook to do is to get people's permission before they apply facial recognition technology to photos?
> A: Yes.
> Q: And because you don't know how Facebook might be able to get that kind of permission, are you saying—it is your testimony that if Facebook is able to get permission consistent with the statute, that Facebook upon getting that permission could apply facial recognition technology to non-users?
> [Re-stating the question after an objection caused Mr. Zellmer to lose his train of thought]
> A: Yes.[56]

Reasonable compliance is possible, as demonstrated here. Moreover, Facebook should be affirmatively enjoined to implement the above procedures. At the very least, there are a multitude of disputed material facts concerning Facebook's ability to comply. Facebook's MSJ must be denied.

E. Injunctive Relief

The MSJ makes a half-hearted pass at arguing injunctive relief is unavailable, stating that Plaintiff cannot establish the elements of injunctive relief, because Plaintiff "has not raised a

[56] Ex.19, Zellmer Tr. 117:19-25;118:1-20.

genuine dispute of fact that would allow him to proceed to trial in his claim for injunctive relief." MSJ, p. 21. Such a throwaway presentation does not begin to carry Facebook's burden on a motion for summary judgment and cannot be taken seriously. Moreover, injunctive relief plainly would be warranted if Plaintiff prevailed.

Whether to award injunctive relief "generally requires a court to consider (1) whether the plaintiff has suffered or will suffer irreparable injury, (2) whether there are inadequate remedies available at law to compensate for the injury, (3) the balance of hardships, and (4) the public interest." *Sierra Club v. Franklin County Power of Ill., LLC*, 546 F.3d 918, 935 (7th Cir. 2008). A complete four-part analysis is not even necessary "when a plaintiff prevail[s] on the merits of his claim, or when, in an action for a statutory injunction, a violation was demonstrated and there [i]s a reasonable likelihood of future violations." *Id.* (citation omitted). Nor is it necessary to balance equities "where the defendant's conduct has been willful." *Id.*

Here, Plaintiff will suffer irreparable injury unless and until injunctive relief is awarded. The Court has the power to order Facebook to alter its practices. All four factors favor injunctive relief. It is Plaintiff's right, not Facebook's, to decide whether to allow the creation, use, collection, and exploitation of his biometric identifiers, and for Facebook to arrogate that decision to itself works irreparable harm. Plaintiff cannot be made whole by any remedy at law because he does not wish to subject his rights of privacy to Facebook's whims. The hardship is entirely on Plaintiff, as Facebook could easily stop its unlawful conduct within the State of Illinois, for example by turning off face scanning for devices with Illinois IP addresses unless the user affirms that they have the consent of every person depicted in the photo, just as Amazon does. Facebook could also require Illinois users to affirm, prior to uploading a photo, that the photo contains only the user's face. Compliance would impose no more than a proportionate and reasonable burden on Facebook compared to the ongoing flouting of Plaintiff's right under Illinois law. And the public interest overwhelmingly favors injunctive relief. Abuses of consumers' privacy by technology giants have made headlines and summoned industry titans to testify before Congress.

Yet Facebook continues to openly flout the State of Illinois' policy judgment that compliance with BIPA is required before Facebook obtains a resident's biometric identifiers. Moreover, the four factors will likely fade in relevance as this case proceeds. The four-part analysis will not even be necessary if Plaintiff prevails on the merits (he will), if a statutory violation is demonstrated and found likely to continue (it is continuing), or if the defendant's conduct is willful (which it is).

IV. CONCLUSION

For the foregoing reasons, Facebook's motion for summary judgment should be denied in its entirety.

Dated: June 10, 2021

Respectfully submitted,

By: */s/ David P. Milian*

David P. Milian*
Email: dmilian@careyrodriguez.com
John C. Carey*
Email: jcarey@careyrodriguez.com
Jennifer M. Hernandez*
Email: jhernandez@careyrodriguez.com
Secondary: ecf@careyrodriguez.com
CAREY RODRIGUEZ MILIAN, LLP
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Telephone: (305) 372-7474
Facsimile: (305) 372-7475
**Admitted pro hac vice*

Bottini & Bottini, Inc.
Albert Y. Chang (SBN 296065)
7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
Telephone (858) 914-2001
Facsimile: (858) 914-2002
Email: achang@bottinilaw.com

Counsel for Plaintiff Clayton P. Zellmer